



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,123	06/30/2000	Martin J. Pagel	1817P	1033

7590 02/09/2004

Sawyer Law Group LLP
PO Box 51418
Palo Alto, CA 94303

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 02/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Page 2

Office Action Summary	Application No. 09/608,123	Applicant(s) PAGEL, MARTIN J.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2,3</u> | 6) <input type="checkbox"/> Other: |

DETAILED ACTION

1. Pursuant to USC 131, claims 1-31 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: on page 4, line 15, the phrase: associated with “on” should be: associated with --one-- also, on page 23, on the abstract, the same mistake needs to be corrected. On page 14, line 8, “rather one” the word --than-- is missing.

Appropriate correction is required.

Claim Objections

3. **Claims 2, 11, 20 and the intervening claims** are objected to because of the following informalities: the word “and” is repeated. Appropriate correction is required.

Claim 1 and the intervening claims are objected to because of the following informalities: On line 13, a “media” should be replaced with a --medium-- .

Claim 4 recites “the method of claim 4”. To avoid rendering the claim indefinite, the dependency of claim 4 needs to be corrected. Examiner will interpret it as dependent on claim 3.

Art Unit: 2136

Claims 10, 19 and the intervening claims are objected to because of the following informalities: a computer readable "media" should be replaced with a computer readable --medium-- . Also, lines 4 and 14 need to be corrected. On line 11, "on" should be --one--. Applicant's cooperation is requested to review the entire application to correct such errors.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1, 7, 10, 16, 19, and 25** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,546,377 to **Gravell et al.**

Art Unit: 2136

4.2 **As per claims 1, 10, and 19, Gravell et al.** substantially teaches method for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups, each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the method comprising the steps of: (a) receiving a plurality of digital token that meets the recitation of verification keys, wherein each one of the received verification keys is encrypted as a function of a respective geographic designation (see column 5, lines 10-17). **Gravell et al.** also discloses receiving a plurality of PSA identification that meets the recitation of key IDs and is encrypted as a function of the same geographic designation used to encrypt the corresponding “digital token” or verification key (see column 5, lines 1-17); (c) in response to receiving a request to generate an indicium for a medium destined for a particular one of the establishments, evidencing the indicium by (i) generating one of the verification keys and the corresponding key ID assigned to indicia generating device's group based on the geographic designation associated with the particular establishment (see column 5, lines 1-17), and (ii) using the generated verification key to create a digital signature, and digitally signing the indicia by including the digital signature and the generated key ID in the indicia (see column 10, lines 31-42 and column 5, lines 1-17).

As per claims 7, 16, and 25, Gravell et al. discloses the limitation of generating and printing indicia for tickets (see column 11, lines 18-23).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5.1 **Claims 2-3, 5-6, 8-9, 11-12, 14-15, 17-18, 20-21, 23-24, 26-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,546,377 to **Gravell et al.** in view of US Patent 6,295,359 to **Cordery et al.**

5.2 **As per claims 28, 2, 11, and 20, Gravell et al.** substantially teaches a method for dispensing and evidencing postage indicia by a postage generating device (PGD) in a system having a plurality of PGDs that have been divided into n groups identified by a group designation G_i , $i = 1, \dots, n$, (see column 4, line 66 through column 5, line 12), the method comprising the steps of: receiving a postal value to generate a key that meets the recitation of receiving a secret key K (see column 4, lines 40-45); (b) in response to receiving a request to generate an indicium for a mail piece destined for a particular postal destination $Dest$, generating the indicium (see column 10, lines 27-46); (c) computing a verification key V_i^{Dest} as a function of

Art Unit: 2136

the secret key K_i and the postal destination (see column 4, lines 40-45 and column 6, lines 57-65); (d) generating a key ID I_i^{Dest} as a function of the postal destination (see column 5, lines 1-17); (e) using the computed verification key V_i^{Dest} to create a digital signature for the indicia (see column 10, lines 31-42 and column 5, lines 1-17); and (f) digitally signing the indicia by including the digital signature and the computed key ID I_i^{Dest} on the indicia (see column 10, lines 31-42 and column 5, lines 1-17). **Gravell et al.** does not explicitly mention that the PSA identification (key ID) is generated using a master secret key K . However, generating keys using asymmetric encryption is notoriously well known in the art. **Cordery et al.** in an analogous art teaches (a) receiving a public master key and a key matrix that meets the recitation of receiving a master secret key K and a secret key K_i (see column 6, lines 39-63); and (d) computing a key ID I_i^{Dest} as a function of the master secret key K (see column 6, lines 58-63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Gravell et al.** to provide a master secret key and a secret key and computing the verification keys as a function of the secret key and the postal destination, and computing the key IDs assigned to the group as a function of the master secret key and the postal destination as taught by **Cordery et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Cordery et al.** so as to provide secure processing for generating postal indicia.

As per claims 3, 12, and 21, Gravell et al. discloses the limitation of generating and printing indicia for postage on a mail piece that is to be received at a plurality of distribution centers (see column 4, lines 13-45).

As per claims 5, 14, and 23, Cordery et al. discloses the limitation of verifying the indicia at an originating distribution center (see column 7, lines 1-12).

As per claims 6, 15, and 24, Gravell et al. discloses the limitation of using zip codes to represent the geographic designations (see column 6, lines 57-65).

As per claims 8, 17, and 26, Gravell et al. substantially teaches distributing to each mailer keys that were encrypted as a function of the geographic designation associated with the establishment. **Gravell et al.** does not explicitly teach distributing keys to each one of the establishments. **Cordery et al.** in an analogous art teaches distributing keys to individual verifying sites (see column 6, lines 45-49 and 59-63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Gravell et al.** to distribute to each one of the establishments the verification keys and the key ID's that were encrypted as a function of the geographic designation associated with the establishment as taught by **Cordery et al.** This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Cordery et al.** so as to provide each one of the establishment keys to verify the signature on the mailpiece.

As per claims 9, 18, and 27, Cordery et al. discloses the limitation of verifying the indicia upon receipt at the particular establishment by using the key ID on the indicia and the

Art Unit: 2136

distributed verifications keys to compute a digital signature, and comparing the computed digital signature with the digital signature on the indicia (see column 7, lines 1-12).

As per claims 29 and 31, **Gravell et al.** substantially teaches computing keys as a function of the PGD designation and a designation of the postal destination (see column 5, lines 10-13 and column 6, lines 53-65). **Gravell et al.** does not explicitly teach using a one-way function. Computing key using a one-way function is well known in the art. **Cordery et al.** in an analogous art teaches computing keys with a one-way function (see column 5 line 35 et seq.) and computing key ID's as a one-way function of the master secret key K (see column 6, lines 39-63). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Gravell et al.** to compute each verification key V_i^{Dest} as a one-way function H of the PGD group key K_i and a designation of the postal destination: $V_i^{Dest} = H(K_i, Dest)$ and computing each of the key ID's as a one-way function H of the PGD group, G_i , the master secret key, K , and a designation of the postal destination, $Dest$: $I_i^{Dest} = H(K, Dest, G_i)$ as taught by **Cordery et al.** to provide secure processing for generating postal indicia. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Cordery et al.** so as to provide secure processing for generating postal indicia.

As per claim 30, **Gravell et al.** discloses the limitation of using ZIP codes to designate the postal destination (see column 6, lines 53-65).

Art Unit: 2136

6. **Claims 4, 13, and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,546,377 to **Gravell et al.** in view of US Patent 6,295,359 to **Cordery et al.** as applied to claims 2-3, 11-12, 20-21 above, and further in view of US Patent 6,005,945 to **Whitehouse**.

6.1 **As per claims 4, 13, and 22**, both references substantially teach generating keys to create a signature and verifying the signature. Neither of the references explicitly teaches verifying the indicia at a destination distribution center. **Whitehouse** in an analogous art teaches discloses the limitation of verifying the indicia at a destination distribution center (see column 27, lines 9-26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Gravell et al.** and **Cordery et al.** as combined above to further include verifying the indicia at a destination distribution center as taught by **Whitehouse** in order to have a wide spectrum of business/operational arrangements. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Whitehouse** so as to have a wide spectrum of business/operational arrangements.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses a multiple device key exchange using asymmetric encryption.

US Patent: 6,636,968

Rosner et al.

Art Unit: 2136

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

February 2, 2004

Ayaz Sheikh
AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100